Worksheet - Number theory and discrete mathematics

Year: University Year 1 · 20

Show your working.

Question 1

Question 1 – The Euclidean algorithm and Bezout *(Section A · Skills practice)*

Let $a = 1071$ and $b = 462$.

a. Use the Euclidean algorithm to find $\gcd(1071, 462)$. [3 marks]
b. Work backwards to write the gcd in the form $1071x + 462y$ with integers x, y. [3 marks]
c. Find $\operatorname{lcm}(1071, 462)$. [2 marks]

Question 2

Question 2 – Inverses and linear congruences *(Section A · Skills practice)*

Work modulo the number given in each part.

a. Find the inverse of 11 modulo 26. [3 marks]
b. Solve $11x \equiv 5 \pmod{26}$. [2 marks]
c. Solve $6x \equiv 4 \pmod{10}$, giving all solutions modulo 10. [3 marks]

Question 3

Question 3 – Fermat and Euler *(Section A · Skills practice)*

Use Fermat's little theorem or Euler's theorem; do not use a calculator for the powers.

a. Find $5^{100} \bmod 13$. [3 marks]
b. Compute $\varphi(360)$. [2 marks]
c. Find the last digit of 7^{222}. [3 marks]

Question 4

Question 4 – The Chinese remainder theorem *(Section A · Skills practice)*

Solve each system of congruences.

a. $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$. [4 marks]
b. $x \equiv 1 \pmod{4}$, $x \equiv 4 \pmod{9}$. [3 marks]

Question 5

Question 5 – Counting techniques *(Section A · Skills practice)*

Answer each counting question, showing the principle used.

a. How many different arrangements are there of the letters of BANANA? [2 marks]
b. In how many ways can a committee of 4 be chosen from 12 people? [2 marks]
c. How many integers from 1 to 1000 are divisible by 3, 5 or 7? [4 marks]

Question 6

Question 6 – Degrees, trees and Euler trails *(Section A · Skills practice)*

Answer each part about simple graphs.

a. A graph has degree sequence $4, 4, 3, 3, 2, 2$. How many edges does it have? Does it have an Euler circuit or an Euler trail? [3 marks]
b. A tree has 15 vertices. How many edges does it have? [1 mark]
c. For which n does the complete graph K_n have an Euler circuit? How many edges does K_6 have? [3 marks]

Question 7

Question 7 – Tiling a kitchen floor *(Section B · Real-life practice)*

A kitchen floor is a rectangle 3.36 m by 2.52 m. A builder wants to cover it exactly with identical square tiles, as large as possible, without cutting any tile.

a. Explain why the side of the tile (in cm) must be a common divisor of 336 and 252.
b. Use the Euclidean algorithm to find the largest possible tile.
c. How many tiles are needed?
d. Tiles of that size cost £7.50 each. Find the total cost, and compare with 28 cm tiles at £1.20 each.

Question 8

Question 8 – Postage with two stamps *(Section B · Real-life practice)*

A post office only has 5p and 8p stamps left. A parcel needs exactly 79p of postage.

a. Explain why the equation $5x + 8y = 79$ has integer solutions.
b. Find one solution using $5 \times (-3) + 8 \times 2 = 1$.
c. Write the general solution and list all solutions with $x, y \geq 0$.
d. Show that 27p cannot be made, and explain why every amount from 28p upwards can (the Frobenius number is $5 \times 8 - 5 - 8$).

Question 9

Question 9 – Calendar arithmetic *(Section B · Real-life practice)*

1 January 2027 is a Friday. Days of the week repeat every 7 days, so we work modulo 7 (Friday $= 0$, Saturday $= 1$, ...).

a. 2027 is not a leap year. Use $365 \equiv 1 \pmod 7$ to find the day of the week of 1 January 2028.
b. What day of the week is 100 days after 1 January 2027?
c. 2028 is a leap year. On what day of the week does 1 January 2029 fall?
d. Explain why the same calendar can be reused only after several years.

Question 10

Question 10 – ISBN check digits *(Section B · Real-life practice)*

An ISBN-10 $d_1 d_2 \ldots d_{10}$ is valid when $10d_1 + 9d_2 + 8d_3 + \cdots + 2d_9 + 1 \cdot d_{10} \equiv 0 \pmod{11}$ (the symbol X stands for 10).

Position	1	2	3	4	5	6	7	8	9	10
Digit	0	3	0	6	4	0	6	1	5	?
Weight	10	9	8	7	6	5	4	3	2	1

a. Find the weighted sum of the first nine digits.
b. Find the check digit.
c. A librarian types the 4 in position 5 as a 7. Show that the error is detected.
d. Explain why any single wrong digit is always detected (use that 11 is prime).

Question 11

Question 11 – A toy RSA code *(Section B · Real-life practice)*

Two friends use a small RSA code. The public key is $n = 55 = 5 \times 11$ and $e = 3$.

a. Find $\varphi(55)$.
b. Find the private key d with $3d \equiv 1 \pmod{\varphi(n)}$.
c. Encrypt the message $m = 8$ by computing $c = m^3 \bmod 55$.
d. Decryption computes $c^d \bmod 55$. Explain why this returns 8 and why real RSA uses primes with hundreds of digits.

Question 12

Question 12 – How strong is a password? *(Section B · Real-life practice)*

A website requires passwords of exactly 8 characters, each a lower-case letter (26 choices) or a digit (10 choices).

a. How many passwords are possible?

b. How many contain at least one digit?
c. An attacker can test 10^9 passwords per second. How long does it take to try them all?
d. How many times more passwords are there if upper-case letters are also allowed?

Question 13

Question 13 – Planning a five-a-side league *(Section B · Real-life practice)*

Eight five-a-side football teams play a league where every team plays every other team exactly once. Model the teams as vertices and the matches as edges.

a. Which graph is this? How many matches are played?
b. What is the degree of each vertex, and what does it mean?
c. Each team plays at most one match per evening. Explain why at least 7 evenings are needed.
d. The league adds a ninth team. How many matches now, and why can no evening have all teams playing?

Question 14

Question 14 – The gritter's route *(Section B · Real-life practice)*

A gritting lorry must treat every street of a village exactly once. The junctions A to F and the number of streets meeting at each are shown.

Junction	A	B	C	D	E	F
Degree	2	3	4	2	3	2

a. How many streets are there?
b. Can the lorry start and finish at the depot at A without repeating a street? Explain.
c. Where must the lorry start and finish to treat each street exactly once?
d. The council adds one street to make an Euler circuit possible. Between which junctions should it go?

Question 15

Question 15 – Domino tilings and Fibonacci *(Section C · Problem solving)*

A garden path is a $2 \times n$ strip made of square slabs. It is covered by 1×2 paving stones (dominoes), each placed either across or along the path. Let t_n be the number of tilings.

n	1	2	3	4	5
t_n	1	2	3	5	8

a. Explain why $t_n = t_{n-1} + t_{n-2}$ for $n \geq 3$ by looking at the left end of the strip.

b. Compute t_{10}.

c. Show that the characteristic equation $r^2 = r + 1$ has roots $\phi = \dfrac{1+\sqrt{5}}{2}$ and $\psi = \dfrac{1-\sqrt{5}}{2}$.

d. Prove by strong induction that $t_n \leq 2^{n-1}$ for all $n \geq 1$.

e. Estimate $\dfrac{t_{20}}{t_{19}}$ and explain.

Question 16

Question 16 – A population recurrence *(Section C · Problem solving)*

Ecologists model a population of beetles (in hundreds) by $a_n = a_{n-1} + 6a_{n-2}$ with $a_0 = 1$ and $a_1 = 8$, where n counts seasons.

n	0	1	2	3	4
a_n	1	8	?	?	?

a. Complete the table.
b. Find the roots of the characteristic equation.
c. Find the closed form $a_n = A \cdot 3^n + B(-2)^n$.
d. Check your formula for $n = 4$ and find a_{10}.
e. Describe the long-term growth.

Question 17

Question 17 – How many in the marching band? *(Section C · Problem solving)*

A marching band has between 100 and 300 members. When they march in rows of 4, three are left over; in rows of 5, two are left over; in rows of 7, one is left over.

a. Write the information as three congruences.
b. Explain why the Chinese remainder theorem gives exactly one solution modulo 140.
c. Solve the system step by step.
d. Find all possible sizes of the band.
e. The band leader says there are more than 200. How many members are there?

Question 18

Question 18 – Scheduling exams with graph colouring *(Section C · Problem solving)*

A sixth-form college must timetable six exams: Maths (M), Physics (P), Chemistry (C), Biology (B), Economics (E) and History (H). Two exams that share a student cannot be in the same session. The clashes are listed below.

Exam	Clashes with
M	P, C, H
P	M, C, E
C	M, P, B
B	C, E
E	B, H, P
H	E, M

a. Draw the clash graph and count its edges using the handshaking lemma.
b. Explain why at least 3 sessions are needed.
c. Give a timetable with 3 sessions.
d. What is the chromatic number of the graph?
e. A new student takes both Biology and History. Can 3 sessions still be used?

Question 19

Question 19 – Proofs by induction *(Section C · Problem solving)*

Mathematical induction is the main tool for proving statements about all natural numbers. Prove each statement for all integers $n \geq 1$ and test it numerically first.

n	1	2	3	4
$7^n - 1$	6	48	342	2400
$3^{2n} - 1$	8	80	728	6560

a. Check that every entry in the table has the divisibility claimed below.
b. Prove that 6 divides $7^n - 1$.
c. Prove that 8 divides $3^{2n} - 1$.
d. Prove that $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$.

Question 20

Question 20 – Challenge: factorials and primes *(Section D · Challenge)*

Factorials contain many prime factors. Legendre's formula says that the power of a prime p in $n!$ is $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.

a. Find the highest power of 2 dividing $50!$.
b. How many zeros does $100!$ end with? And $1000!$?
c. Check Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$ for $p = 7$ and $p = 11$.
d. Show that $(n-1)! \equiv 0 \pmod{n}$ when $n = ab$ with 1, so Wilson's congruence characterises primes (apart from $n = 4$).